

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/8/2008 has been entered.

### ***Examiner's Amendment***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Raymond E. Roberts (Reg. No. 38,597) on 29 August 2008.

This application has been amended as follows:

IN THE CLAIMS

**Replace claim 1, 11 and 20 as follows.**

Art Unit: 2131

**CLAIM 1:**

A computer program, embodied on a computer readable storage medium, for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, comprising:

a code segment that listens with a computerized system for an activation of the hyperlink;

a code segment that extracts an originator identifier and encrypted data from the hyperlink, wherein said encrypted data associated with said hyperlink does not include payload data;

a code segment that decrypts said encrypted data into decrypted data based on said originator identifier;

a code segment that matches said originator identifier from said hyperlink to one of a plurality of registered originators against a unique identity extracted from said decrypted data;

a code segment that presents information on a display unit;

a code segment that redirects; and

a code segment that determines whether the hyperlink includes said originator identifier and said encrypted data decrypts successfully, and then:

runs said code segment that presents, to present a confirmation of authentication to the user conveying the name of an owner and the domain name of the target URL, and

runs said code segment that redirects, to redirect the user to the target URL;

and otherwise, runs said code segment that presents, to present a warning dialog to the user.

Art Unit: 2131

**CLAIM 11:**

A system for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the system comprising:

a computerized system having a display unit;

a logic in said computerized system that listens for activation of the hyperlink;

a logic that extracts an originator identifier and encrypted data from the hyperlink,

wherein said encrypted data associated with said hyperlink does not include payload data;

a logic that decrypts said encrypted data into decrypted data based on said originator identifier;

a logic that matches said originator identifier from said hyperlink to one of a plurality of registered originators against a unique identity extracted from said decrypted data;

a logic that determines whether the hyperlink includes said originator identifier and that said encrypted data decrypts successfully;

a logic responsive to said logic that determines, that presents on said display unit a confirmation of authentication conveying the name of the owner and the domain name of the target URL and that redirects the user to the target URL; and

a logic responsive to said logic that determines, that presents on said display unit a warning dialog to the user.

**CLAIM 20:**

A method for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the method comprising:

Art Unit: 2131

listening for an activation of the hyperlink;

extracting an originator identifier and encrypted data from the hyperlink, wherein said encrypted data associated with said hyperlink does not include payload data;

decrypting said encrypted data into decrypted data based on said originator identifier;

matching said originator identifier from said hyperlink to one of a plurality of registered originators against a unique identity extracted from said decrypted data;

when the hyperlink includes said originator identifier and said encrypted data decrypts successfully:

presenting a confirmation of authentication to the user, wherein said confirmation of authentication conveys the name of an owner and the domain name of the target URL; and

redirecting the user to the target URL;

and otherwise, presenting a warning dialog to the user.

### ***Allowable Subject Matter***

Claims 1 – 8, 10 – 17 and 19 – 24 and 26 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 1, 11 and 20 (& associated dependent claims).

The present invention is directed to a method for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the method comprises listening for an activation of the hyperlink; extracting an originator identifier and encrypted data from the hyperlink, wherein said encrypted data associated with said hyperlink does not include payload data. The closest prior arts on the record, either singularly or in combination fails to anticipate or

Art Unit: 2131

render obvious the claimed invention that decrypting said encrypted data based on said originator identifier, into decrypted data and matching said originator identifier from said hyperlink to one of a plurality of registered originators against a unique identity extracted from said decrypted data; when the hyperlink includes said originator identifier and said encrypted data decrypts successfully: presenting a confirmation of authentication to the user, wherein said confirmation of authentication conveys the name of an owner and the domain name of the target URL; and redirecting the user to the target URL

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

/Longbit Chai/

Longbit Chai Ph.D.  
Primary Patent Examiner  
Art Unit 2131  
9/6/2008